☑002

2

PATENT APPLICATION
USSN 10/658,345
Attorney Docket No.: VDAN-40003

Remarks

The Examiner's rejection of claims 1-8 under 35 U.S.C. § 102(b) for being anticipated by the Ozzie U.S. Patent No. 5,664,099, as this rejection may be attempted to be applied against the claims, is respectfully traversed.

In support of this traverse it is noted that from a first view of Ozzie and the subject application there appears to be a great similarity between Ozzie et al. U.S. Patent No (5,664,099) and the present application, but at a closer look, the two are totally different.

Before dealing in detail with point 4 of the action, wherein applicant's claim 1 is cited and alleged as being disclosed at Ozzie, let us first give a short comparative explanation what Ozzie does and what is considered as the corresponding part of the present application. Following this explanation, the differences will be more apparent.

1. Ozzie wishes to establish a protected channel between a user and a computer system in response to a user request. Ozzie wishes prevention against the following two dangers: (i) the user's computer has been accesses by a pirate (non authorized) source other than the correct remote computer system, and (ii) the unauthorized persons cannot learn how an access to the system can be obtained.

2. Ozzie's user has to enter a multi-digit predetermined and pre-stored password whereas the user has to observe the display and as the typing of the password continues, a predetermined pattern should be seen on the screen, which should step-wise change appearance after certain characters have been typed.

3

3. The user and the system must know in advance not only the correct password but also the unique individual patterns and as it is changed when the typing process goes on.

4. When the program displayed comes from a non-authorized source which cannot know and generate the predetermined pattern, the user notices it (i.e. that the pattern differs from the one he has learned) and enters a failure code which makes an end to the session.

5. If the patterns are found correct, and the password has been fully typed, the user transits an "end of password" status code to the system, and the system compares the typed password with the stored one and in case of matching provides access to the user.

In this system the above outlined operation is connected with certain properties, as follows:

a. The user must learn the specific patterns, i.e. the one displayed at the beginning of the session and the individual further discrete changed versions as the typing of the password goes on.

b. The whole pattern recognition process is tied to the typing of the password by the user.

c. The system must store the predetermined sequences of unique patterns and send them to the user as the typing goes on.

d. At a version the pattern is generated in specially coded way from one or more fractions of the password, however, the user must know these specific patterns as well.

4

In contrast to these properties, the present application has different properties:

1. The present application is an authorization method for providing access for an enrolled user to a limited access system, wherein the system has an authorization centre and a remote location. (*The difference here to Ozzie is: (i) that applicant's method does not care about any possible danger of an intruding unauthorized program, and (ii) the authorization is granted exclusively by the authorization centre, the user is not given any right to decide*)

2. Applicant's user has to enter either an identification code or a password for temporarily identifying himself, which even if correct does not result the granting of an access. (*The difference to Ozzie is that the identification of the user precedes the subsequent authorization process and the two are not tied and the authorization process is fully independent from the password typed by the user*).

3. Neither the system nor the user has to learn any predetermined pattern, and such patterns are therefore not stored in the system, and no unique pattern is associated with the user and with its password. What both the user and the system have to learn is a rule (this was called in the specification as: "symbol set selection algorithm) which defines how certain patterns have to be selected from a plurality of displayed patterns. (*Difference: for humans it is much easier to learn a rule of selection than to remember certain complex patterns. Such a rule can be e.g. "select the element which has the darkest color from the second row from the top"*).

4. Following the identification of the user, the authorization centre sends a non-unique display picture to the user which comprises a plurality of elements, wherein the specific rule learnt by the user can be applied. The user has now a task to apply the rule and to select the elements that comply with the rule. This

5

selection as the user's response is sent to the authorization centre. The authorization centre which knows the display picture sent originally to the user applies the rule (as the rule is stored therein) and generates a correct selection. This locally generated selection (made by the computer) is compared with the selection received from the user, and access is granted if the two selections are identical. (*Differences: (i) the user must make a selection by applying the rule and he does not have to establish whether a displayed picture is the same as the one he remembers. (ii) the authorization centre generates the same selection by applying the rule, and compares it with the response of the user*

5. The selection of the patterns by applying the rule is the end of the job what the user has to do, from this time onward, the authorization centre works, and decided to grant access to the user. (*In the known system the user must type in the end of password message*).

The above outlined differences demonstrate that the method of Ozzie is completely different from the present application.

The question now presented is how can applicant prove on that basis that point 4 of the action is non-supported.

Applicant will show clause by clause that the concerned clause can be found at Ozzie or not.

1. "Assigning an identification code to said user and storing the assigned identification code at the authorization centre" Comment: This **is true** for Ozzie.

6

2. "Assigning a symbol set selection algorithm to said user". Comment: This is **not true** for Ozzie. In column 5 Lines 25 -37 at Ozzie it can be read that "the code produces a unique graphical pattern on the password entry screen for each user of the system", furthermore "a unique display pattern is generated from the new ID code". These statements of Ozzie define that a unique pattern is generated from the code at Ozzie, and this is stored. From Ozzie's specification it is also clear that the user must learn this unique pattern so that later he should be able to determined if a displayed pattern is different from the one he has learned. The assignment of a "rule" i.e. "symbol set generation algorithm" with the user is different from the assignment of a unique pattern. The unique pattern is always the same. The "rule" can be applied at several displayed picture that comprises predetermined elements. In that case, the initial displayed picture can be different at all cases, and the resulting selection is also different. This is a basic difference from Ozzie, as the user does not have to learn any pattern, and the originally displayed pattern can be different even in case of the same user. Furthermore, the selected pattern always will be different, unlike at Ozzie, wherein as the typing proceeds, always the same patterns are displayed. A clever intruder can therefore learn the always same patterns.

3. "storing the assigned symbol set selection algorithm at the authorization centre in association with the identification code of the user". Comment: This allegation **is not true for Ozzie**, as there the pattern is stored and not the "rule of selection"

4. "Wherein the symbol set selection algorithm being a list of instructions how a predetermined number of graphic symbols can be generated from a table of graphic symbols". Comment: This is **also not true for Ozzie**,

wherein the pattern generated is associated with and generated from the password. In Ozzie, the user is not informed on the way how a selection can be made from the table of patterns, moreover Ozzie's users do not have to make any selection, the user must only type the password and see the screen to establish whether the displayed pattern is the same as what he has learned.

5. "wherein each graphic symbol is characterized by a predetermined number of dominant features and each dominant feature can take a number of values". Comment: This feature **is not disclosed** at Ozzie. Column 5, lines 26-37 define only that a unique pattern is generated from the new ID code. This cannot involve that the graphic symbols forming the pattern each must have dominant features that can take one of several values (i.e. colors, shades, edges, corners, etc.). The user of Ozzie must remember and recognize a pattern, whereas applicant's user need not recognize a pattern which is displayed to him, but he must be able to apply the rule on the graphic symbols within the display pattern by watching these properties of the elements.

6. "Displaying for said user on said remote terminal a table of randomly chosen different graphic symbols so that the user can apply the assigned symbol set algorithm for generating a predetermined number of generated symbols". Comment: This *is not true* for Ozzie. According to column 4, lines 49-47, the elements (characters) of the password typed by the user are utilized for the non-unique generation of a pattern of icons. The difference lies in, that at Ozzie this operation is made by the system and the system generates from the typed characters the specific transformed pattern (which has to be memorized and known by the user), while according to the present citation from applicant's claim 1, it is the user who

8

should apply the "rule" to make the selection from the displayed table. At Ozzie, the user does not have to make any selection and to apply any rule for a selection.

7.   "forwarding said generated symbols to said authorization centre". Comment: This is **not true** for Ozzie, as the user does not forward any symbol set to the centre.

8.   "forwarding said user identification code from the remote terminal to the authorization centre". Comment: This is **partially true** at Ozzie, but in applicant's method the sending of the identification code to the authorization centre need not occur at the beginning of the dialog between the centre and the user as it is necessary at Ozzie, because otherwise the system would not be able to transmit the pattern unique to the identified user. In applicant's system, the identification can be given just before the remote system generates to rule on the transmitted pattern.

9.   "at the authorization center using the received identification code and reproducing said generated symbols by using the selection algorithm associated with the identified user". Comments: This is **not true** for Ozzie. There, when the typing of the password is finished, the user has the right to inform the system that the patterns were not the one he expected (step 616, 626, 630: N output). Otherwise, when the password has been typed, step 632 (Fig. 6B) is carried out, the system checks the typed password with the stored password (Column 7, lines 10-11). This is a simple comparison of two sets of characters. In this cited clause, the system itself reproduces the generated symbols by applying the agreed rules on the initial table of patterns.

10. "and comparing the locally reproduced response symbols with the ones received from the remote terminal and providing access to said user only if

9

the received and generated symbols being identical." Comment: This is not true at Ozzie, since there the stored password is compared with the entered password, while in the present application the locally generated symbols are compared with the symbols generated and sent by the user.

From this explanation one can see that the Examiner has misinterpreted the present invention and considered Ozzie's specification as one fully anticipating applicant's claim 1. The difference is substantial, in that claim 1 not only differs from Ozzie but also is not obvious from the teaching included in Ozzie.

The dependent claims 2-8 are considered patentable over Ozzie for the same reasons that claim 1 is considered patentable over Ozzie and for the reason that each of these claims further limits the authorization method of claim 1.

The Examiner's rejection of claims 9-11 under 35 U.S.C. § 103 (a) for being unpatentable over the Ozzie U.S. Patent No. 5,664,099 in of the Patzer et al. U. S. Patent No. 6,732,2760, as this rejection may be attempted to be applied against the claims, is respectfully traversed.

In support of this traverse, it is noted that the content of claims 9 to 11 go an important step further over claim 1, namely after the access has been provided to the remote user, the transmission of substantial information (message) between the center and the so authorized user is also ciphered, and the same transformation and ciphering technique is used as at the user-authorization. In Ozzie, the message is left out of attention. Claims 9 to 11 are therefore especially inventive in addition to the patentability of claim 1, set forth above, and over Patzer et al. which merely authenticates a network server to an authentication server.
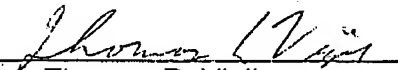
☑010

10

In summary, applicant submits that, for the reasons set forth above, the claims are clear of the art of record and otherwise in condition for allowance. An early and favorable action to that end is requested.

Respectfully submitted,

June 19, 2007
Chicago, IL 60601
221 N. LaSalle Street
Room 2036
(312) 236 8123

Pyle & Piontek, LLC

By _____
Thomas R. Vigil
Registration No. 24,542